UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

JILLIAN CANTINIERI, on behalf of herself and all others similarly situated,

Plaintiff,

-against-

VERISK ANALYTICS, INC., INSURANCE SERVICES OFFICE, INC., and ISO CLAIMS SERVICES INC.,

Defendants.
----------X

ORDER

21-CV-6911 (JMA)(JMW)

A P P E A R A N C E S:

Anthony Pasquale Mastroianni, Esq.
Jerrold S. Parker, Esq.
Raymond C. Silverman, Esq.
Parker Waichman LLP
6 Harbor Park Drive
Port Washington, NY 11050
Attorneys for Plaintiff

Jasmeet Ahuja, Esq.
Hogan Lovells US LLP
1735 Market Street, 23rd Fl.
Philadelphia, PA 19103
Attorney for Defendants

Allison M. Holt-Ryan, Esq.
Joseph J. Cavanaugh, Esq.
Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, DC 20004
Attorneys for Defendants

WICKS, Magistrate Judge:

Before the Court is the parties' joint status report raising for the Court's consideration discovery disputes that arose out of the court-ordered deposition of Michael Snook. (ECF No. 63.) In essence, Plaintiff Jillian Cantinieri seeks to compel certain discovery which Defendants Verisk Analytics, Inc. ("Verisk"), Insurance Services Office, Inc. ("ISO"), and ISO Claims Services Inc. ("ISOC") resist. In fact, at this juncture, Defendants request that the Court close the shades on the limited jurisdictional discovery that was referred to the undersigned by the Hon. Joan M. Azrack. As a result of the issues raised in the joint status report, the Court construes the report as Plaintiff's motion to compel and Defendants' cross-motion for a protective order.

For the reasons stated below, these motions are granted in part and denied in part.

I. BACKGROUND

Given the prior Orders in this case, the Court assumes the parties' familiarity with the background and procedure and repeats it here only to the extent relevant to the focused jurisdictional discovery ordered and the instant dispute. Plaintiff brings a putative class action against Defendants alleging negligence, negligence *per se*, and violations Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 and New York General Business Law § 899-aa and § 349. (ECF No. 1.) Plaintiff's grievance revolves around Defendants' failure to safeguard certain personally identifiable information submitted to them by Plaintiff's insurer. (*Id.*) Defendant ISOC's November 4, 20221 letter ("Notification Letter") to Plaintiff notified her could have been impacted in a data breach suffered by ISOC. (ECF No. 29 at 2.) The Notification Letter noted that as early as July 5, 2021 an unauthorized entity got a hold of customer credentials and accessed the customer portal -- ExpressNet portal -- and obtained motor vehicle reports available through the portal that contain driver's names, dates of birth, addresses,

and license numbers. *Id*. Plaintiff's dispute the timing and scope of the data breach and posit that the breach could have occurred earlier than Defendants represent and involved more information that they claim, such as social security numbers.

On March 31, 2023, Judge Azrack denied Defendants' 12(b)(1), (6) motion to dismiss Plaintiff's complaint without prejudice. (ECF No. 49.) Judge Azrack directed focused jurisdictional discovery to resolve whether Plaintiff has Article III Standing and noted that Defendants would be permitted to renew their motion following such discovery. (*Id*. at 4.) After all, if the earliest date of access was July 5, 2021, any of Plaintiff's injuries prior to that date could not confer constitutional standing since they could not be said to be fairly traceable to the security incident. (*Id*. at 3.) The same would be true if the security incident did not, or could not have, involved the disclosure of information like social security numbers which relate to and could have caused Plaintiff's injuries. (*Id*.) Judge Azrack found jurisdictional discovery warranted on the following:

> (1) the timeframe of the data breach and (2) the data elements exposed or obtained in the data breach. Subsidiary facts relevant to the latter point include: (1) the specific data elements Plaintiff disclosed to her insurance company, (2) the specific data elements that her insurance company disclosed to Defendants, and (3) the specific data elements that were exposed or obtained in the breach.

(*Id*. at 4–5.)

Subsequently, on May 9, 2023, the parties appeared before Judge Azrack to further discuss the focused jurisdictional discovery. (ECF No. 52.) Jurisdictional discovery was referred to the undersigned to oversee the discovery process, which Judge Azrack anticipated to be completed within 45 days *limited* to the following issues:

> First, whether Plaintiff's Social Security number ("SSN") was disclosed as part of the security incident; and second, when the security incident occurred. Regarding the first issue, Defendants shall provide access to [ExpressNet] portal(s) in question so that Plaintiff may evaluate Defendants' representation that the security

> incident did not result in disclosure of Plaintiff's SSN. Regarding the second issue, Defendants shall provide the factual basis for Crowdstrikes conclusion that the security incident began no earlier than July 5, 2021.

(ECF No 51.)

On May 17, 2023, the parties appeared before the undersigned for a status conference where Defendants were directed to product documents forming the factual basis for Crowdstrike's (Defendants' third-party vendor) conclusion that the security incident started no earlier than July 5, 2021. (ECF No. 52.) A dispute arose around the level of access Defendants were to provide Plaintiff with respect to the ExpressNet portal. (*Id*.) That dispute was resolved at a subsequent status conference on June 14, 2023 where the parties were advised that based on conversations with Judge Azrack's chambers, the level of access Plaintiff outlined in the joint status report (ECF No. 57) is in line with the level of access to be provided. (ECF No. 56.) That is, Defendants were to provide a demonstration of the ExpressNet portal to Plaintiff. (*Id*.) Accordingly, the parties were directed to complete the demonstration on or before June 23, 2023 (*Id*.)

Further, as to the factual basis for Crowdstrike's conclusion regarding the earliest point of unauthorized access, the parties continued to disagree as to whether Defendants had provided enough documentation to satisfy the discovery ordered. (*Id*.) Having heard the parties' positions and reviewed items screenshared by Defendants' counsel, an in-person conference was scheduled to determine whether any further discovery was needed. (*Id*.) The parties were directed to bring any discovery that had been exchanged, that they believe supported their respective positions, and any consultants or demonstratives that could aid them in explaining those positions. (*Id*.) Given the continuing dispute, and the parties' and the Court's schedules,

the Court directed the parties to continue jurisdictional discovery beyond the 45-day mark (June 23, 2023) unless Judge Azrack ordered otherwise. (ECF No. 56.)

The parties appeared for the in-person conference on July 19, 2023 at which time they advised the Court of the status of jurisdictional discovery and stated their respective positions on the need for further discovery. (ECF No. 59.) In the interim, the parties had also raised certain issues that arose during the demonstration of the ExpressNet portal. (ECF No. 57.) These were also addressed at the July 19, 2023 conference. The Court, for the reasons stated on the record, overruled Plaintiff's objections to Defendants' demonstration of the ExpressNet portal.

The Court also permitted Plaintiff to conduct a limited deposition of Michael Snook, that is, the witness who verified Defendants' responses to Plaintiff's interrogatories. (ECF No. 59.) And as agreed amongst counsel, "the deposition [was to] be limited to the interrogatory responses and the two jurisdictional issues and shall not exceed two hours. [And] Counsel [were] reminded that merits discovery is off-limits." (*Id.*). The two jurisdictional issues being whether Plaintiff's social security number was impacted in the security incident and the factual basis for Crowdstrike's determination that the earliest unauthorized access date was July 5, 2021. The parties were to complete the deposition on or before August 4, 2023 and file a joint status report regarding the same on or before August 11, 2023. (*Id.*) The Court granted the parties' consent motion to extend these deadlines by one week. (ECF No. 61.)

On August 18, 2023, the parties filed the instant joint status report, which outlines their remaining disputes, and is in substance a motion to compel and a cross-motion for a protective order. (ECF No. 63.) Defendants request that jurisdictional discovery be deemed closed, whereas Plaintiff seeks to compel (i) responses to certain questions asked at the deposition that

Defendants objected to, and (ii) a supplemental response to Interrogatory No. 17 based on the deposition testimony. (*Id.*)

II. LEGAL STANDARD

"Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case" but that determination involves weighing certain factors such as the importance of issues, amount in controversy, relative access to information, resources, importance of the discovery sought in resolving issues, and "whether the burden or expense" of the discovery trump its "likely benefit." Fed. R. Civ. P. 26(b)(1). Rule 37(a)(3)(B), permits a party seeking discovery to "move for an order compelling an answer, designation, production, or inspection." Fed. R. Civ. P. 37(a)(3)(B).

A motion to compel may properly be made where, for example, "a deponent fails to answer a question asked under Rule 30 or 31 . . . [or] a party fails to produce documents or fails to respond that inspection will be permitted . . . as requested under Rule 34." Fed. R. Civ. P. 37(a)(3)(B). It is beyond peradventure that "[m]otions to compel are left to the court's sound discretion." *Mirra v. Jordan*, No. 13-CV-5519 (AT)(KNF), 2016 WL 889683, at *2 (S.D.N.Y. Feb. 23, 2016); *see also Liberty Mut. Ins. Co. v. Kohler Co.*, No. 08-CV-867 (SJF)(AKT), 2010 WL 1930270, at *2 (E.D.N.Y. May 11, 2010) ("[A] motion to compel is entrusted to the sound discretion of the district court.").

On the other hand, parties seeking cover from discovery may avail themselves of a motion for a protective order which, in effect, is the flip side of a motion to compel. Rule 26(c) affords protection for abusive or embarrassing discovery, providing that "[a] party or any person from whom discovery is sought may move for a protective order in the court where the action is

pending . . . The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense. . . ." Fed. R. Civ. P. 26(c)(1); *see Gordon v. Target Corp.*, 318 F.R.D. 242, 246 (E.D.N.Y. 2016) ("[T]he touchstone for determining whether to issue a protective order under Rule 26(c) lies, in the first instance, on a party's ability to establish good cause").

"If the movant establishes good cause for protection, the court may balance the countervailing interests to determine whether to exercise discretion and grant the order." *Rofail v. United States*, 227 F.R.D. 53, 55 (E.D.N.Y. 2005). "Because of the interest in broad discovery, the party opposing the discovery of relevant information, whether through a privilege or protective order, bears the burden of showing that based on the balance of interests the information should not be disclosed." *Fowler-Washington v. City of New York*, No. 19-CV-6590 (KAM)(JO), 2020 WL 5893817, at *3 (E.D.N.Y. Oct. 5, 2020) (internal quotation and citation omitted). It is against this backdrop that the Court considers the present application.

III. DISCUSSION

Defendants request that jurisdictional discovery be deemed closed, whereas Plaintiff seeks to compel further discovery. These issues fall neatly into two categories of information that Plaintiff seeks: (i) responses to the three questions Defendants objected to during Snook's August 9, 2023 deposition, and (ii) a supplemental response to Interrogatory No. 17 based on information purportedly learned during Snook's deposition. (*Id.*). Each category is addressed below.

A. Scope of Deposition

The first dispute relates to Defendants' objections to the following three questions posed by Plaintiff during Snook's deposition:

> "Q. As of April 2021, did the defendants store or maintain plaintiff's Social Security number or personal identifying information on any of its networks, systems or databases?" Deposition transcript of Michael Snook (August 9, 2023)["Snook. Tr.], pg. 44, lns. 4-8.
>
> "Q. As of April 2021, did the defendants store or maintain plaintiff's financial information or insurance claim information on any of its networks, systems or databases?" Snook. Tr. at 48:18-21.
>
> "Q. To your knowledge, Mr. Snook, did plaintiff's insurance company ever disclose plaintiff's Social Security number or other personal identifying information to the defendants at any time?"

(ECF No. 63 (citing Snook Tr. at 49:3-7).)[1]

Plaintiff argues that these questions are well within the scope of Interrogatory No. 16, and that when the parties agreed upon the scope the interrogatories at issue for deposition, they agreed to include Interrogatory No. 16. (ECF No. 63 at 1.) Further, Plaintiff argues that this line of questioning is within the ambit of the focused jurisdictional discovery ordered by Judge Azrack. (*Id*. at 2.) Defendants raise two objections. First, in Defendants' view, the undersigned directed a deposition limited to interrogatory *responses* and the two jurisdictional issues, not the interrogatory request itself. (*Id.* at 4 (citing ECF No. 59).) Second, Defendants argue that Plaintiff's questions are (i) outside the scope of jurisdictional discovery ordered by Judge Azrack, (ii) that Judge Azrack's May 9, 2023 Order superseded her March 31, 2023 Order, and (iii) in any event, the information sought is not even within the scope of the jurisdictional discovery contemplated in the initial March 31, 2023 Order. (*Id*. at 4–5.)

All three questions asked are geared toward one of the "key jurisdictional facts" that Judge Azrack noted required discovery (ECF No. 49 at 4–5), specifically, "the data elements exposed or obtained in the data breach." (*Id*.) Judge Azrack's subsequent order, *inter alia*, allowed Plaintiff to "evaluate Defendants' representation that the security incident did not result

[1] Snook's deposition transcript was not provided.

in disclosure of Plaintiff's SSN." (ECF No 51.) Absent an express intention to the contrary, the second order merely supplements, not supplants, the first. Thus, on their face the questions appear to technically be within the court-ordered jurisdictional discovery. That is, they are consistent with the undersigned's directive that the deposition "shall be limited to the interrogatory responses and the two jurisdictional issues[.]" (ECF No. 59.)

However, there is one important caveat. Plaintiff has not provided any piece of information that establishes the relevance of these questions and the information sought given her prior representations. As Defendants note, Plaintiff represented at the July 19, 2023 status conference that the bad actors at issue here walked through the front door of the ExpressNet portal carrying standard customer credentials rather than by hacking into Defendants' systems. (ECF No. 49; ECF No. 62 at 22 ("Nobody broke in, nobody hacked in. They let them in through the front door and let them take whatever they want provided they paid for it for about three months."). Naturally then, absent a hack or cyber intrusion, only information that could be accessed through the ExpressNet portal would be relevant as far as what data elements were impacted during the security incident. (*Id.*) Therefore, it would not matter what personally identifiable information, if any, was available on any other network, system or database. Of course, if there was some inkling that the entities that fraudulently accessed the ExpressNet portal using customer credentials hacked into other areas, that would change the equation.

Plaintiff asserts these questions are vital since Snook represented that Defendants' investigation into the security incident did not involve looking into whether additional personally identifying information, outside of the information contained in the motor vehicle reports accessible from the ExpressNet portal, could have been exposed or obtained in the security incident. (ECF No. 63 at 2.) Not necessarily so. Sure, the absence of evidence is not the

evidence of absence. But as discussed at the July 19, 2023 conference, Plaintiff's counsel has not provided any basis to make a connection between the customer-level access that the fraudulent entities had to the ExpressNet portal and some sort of cyber intrusion or hack that would have allowed them to access information kept elsewhere. Without that connection, further discovery is simply a shot in the dark.

If it turns out certain personally identifiable information is kept in other parts of Defendants' network, system or database, that kicks open the door to the same kind of exploration the undersigned previously rejected as inquiring into the merits. (*See* ECF No. 62 at 26.) Surely, the Court would soon be faced with requests regarding penetration tests and alike to see whether a hack or cyber intrusion occurred in any of Defendants' networks, systems, or databases. To allow this line of questioning would steer this limited jurisdictional discovery into an impermissible fishing expedition.

These questions are not relevant to the limited jurisdictional discovery, and Michael Snook's deposition is deemed complete. Thus, Plaintiff's application to compel responses is denied, and Defendants are granted a protective order with respect to this line of questioning.

B. Supplemental Response to Interrogatory No. 17

The second dispute pertains to Interrogatory No. 17, which is one of the agreed-upon interrogatories for the scope of the deposition. (ECF No. 63 at 3.) In relevant part, Interrogatory No. 17 provides:

> Describe in detail whether, and if so, how, You determined the earliest date that any PII was accessed during the Data Breach. Your response must include, but not be limited to, what You determined the PII to be, what information was accessed, including the size, scope, and type of the information accessed, and identification of any and all documents containing PII that were accessed without authorization during the Data Breach.

(*Id.*)

Plaintiff seeks a response related to Defendants' internal review of its logs of the interactions between the ExpressNet portal and all users starting from August 2020. (*Id.*) Snook provided testimony regarding this review and its purpose, which was to look for any odd activity to help locate any other fraudulent accounts that may have accessed the ExpressNet portal. (*Id.*) However, Snook was allegedly unable to provide a fulsome response detailing the steps taken by Defendants or Crowdstrike to review the anomalous activity. (*Id.*)

Defendants argue that they have already provided discovery on the exact same topics, and that Snook testified at length about the investigation Defendants undertook regarding the incident. (*Id.* at 6.) Defendants also point to the fact that their internal investigation and Crowdstrike's review both independently came to the same conclusion that there was no unauthorized access before July 5, 2021. (*Id.*) Defendants aver that any further discovery at this juncture would be unreasonably cumulative, unduly broad, overly burdensome, and disproportionate to the needs of this case.

Putting aside these conclusory boilerplate objections, the information Plaintiff seeks must be produced. As Plaintiff notes, the fact that Defendants' review of internal logs dating back to August 2020 was volunteered by Snook in response to questions about the basis for Defendants' conclusion about the earliest date of unauthorized access. (*Id.*) There is no doubt that the Defendants' review of its internal logs to assess the incident, which informed their conclusion regarding earliest point of unauthorized access, is relevant and within the scope of jurisdictional discovery. Moreover, this information is responsive to Interrogatory No. 17 and producing it is hardly burdensome given the parties' ongoing duty to supplement their discovery responses. *See* Fed. R. Civ. P. 26(e)(1)) (duty to supplement discovery responses if the response is incomplete

and the supplemental information "has not otherwise been made known to the other parties during the discovery process or in writing" or "as ordered by the court"); *Neogenix Oncology, Inc. v. Gordon*, No. 14-CV-4427 (JFB)(AKT), 2017 WL 4233028, at *2 (E.D.N.Y. Sept. 22, 2017) ("[A]s new information comes into its possession, the responding party has a continuing duty to supplement their responses.").

Thus, Plaintiff is entitled to a more detailed response to Interrogatory No. 17 that describes the steps taken with respect to Defendants' investigation and Crowdstrike's review of Defendants' internal logs dating back to August 2020. This part of Plaintiff's application to compel is granted, and Defendants' application for a protective order is denied.

CONCLUSION

Accordingly, Plaintiff's motion to compel, and Defendants' cross-motion for a protective order, are granted in part and denied in part.

Defendants shall fully respond to Plaintiff's Interrogatory No. 17 consistent with this Order on or before **September 15, 2023**.

The limited jurisdictional discovery ordered by Judge Azrack on May 9, 2023 is otherwise deemed complete, and the matter is respectfully returned to Judge Azrack for further consideration.

Dated: Central Islip, New York
September 5, 2023

SO ORDERED:

/S/ James M. Wicks

JAMES M. WICKS
United States Magistrate Judge